



АНДРЕЙ ЛЕОНОВ

ИИ АГЕНТЫ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО
ПО ВНЕДРЕНИЮ ИИ-АГЕНТОВ
В БИЗНЕС И ЖИЗНЬ

КЕЙСЫ • ТЕХНОЛОГИИ • ОТРАСЛИ

Андрей Леонов

ИИ Агенты

«Автор»

2026

Леонов А.

ИИ Агенты / А. Леонов — «Автор», 2026

ИИ-агенты уже перестают быть игрушкой для технарей. Это новый слой бизнеса: цифровые исполнители, которые умеют принимать задачу, искать информацию, работать с документами, вызывать программы и API, общаться с людьми и доводить процесс до результата. В книге Андрей Леонов простым языком показывает, где агенты дают деньги и экономят время: B2B и B2G, eCom, EdTech и FinTech, КФХ, производство и роботы, кино и видеореклама, психология и отношения, медицина и здоровье, корпоративные внедрения и другие ниши. Внутри — вопросы для аудита бизнеса, сценарии продаж, кейсы внедрения, архитектуры и технологические стеки. Это книга не про «волшебную кнопку», а про то, как превратить ИИ-агента в понятную рабочую систему с ответственностью, метриками и экономикой.

© Леонов А., 2026

© Автор, 2026

Содержание

Введение. Агент — это не чат-бот	6
Глава 1. Как найти работу для агента	8
Глава 2. Аудит через вопросы и продажи	10
Глава 3. Карта агента: цель, память, инструменты, контроль	12
Конец ознакомительного фрагмента.	19

Андрей Леонов

ИИ Агенты

ИИ Агенты

Андрей Леонов

Практическое руководство по аудиту, продаже, архитектуре и внедрению ИИ-агентов

Содержание

1. Введение. Агент — это не чат-бот — 4
2. Глава 1. Как найти работу для агента — 6
3. Глава 2. Аудит через вопросы и продажи — 8
4. Глава 3. Карта агента: цель, память, инструменты, контроль — 10
5. Глава 4. B2B: агент отдела продаж — 12
6. Глава 5. B2B: поддержка и сервис — 14
7. Глава 6. B2G: документы и обращения — 16
8. Глава 7. eCom: товар, заказ, повторная покупка — 18
9. Глава 8. EdTech: персональный наставник — 20
10. Глава 9. FinTech: деньги любят ограничения — 22
11. Глава 10. КФХ и агробизнес — 24
12. Глава 11. Производство: диспетчер и качество — 26
13. Глава 12. Роботы: агент как диспетчер — 28
14. Глава 13. Кино и сериалы: агентская фабрика — 30
15. Глава 14. Видеореклама — 32
16. Глава 15. Маркетинг и контент — 34
17. Глава 16. Психология: помощник, не диагност — 36
18. Глава 17. Отношения: помощник коммуникации — 38
19. Глава 18. Медицина и здоровье — 40
20. Глава 19. Корпоративное внедрение — 42
21. Глава 20. Архитектуры и технологические стеки — 44
22. Глава 21. RAG и корпоративные знания — 46
23. Глава 22. Мультиагентные системы — 48
24. Глава 23. Безопасность и человеческий контроль — 50
25. Глава 24. Экономика агента — 52
26. Глава 25. Система продаж внедрений — 54
27. Глава 26. Практический аудит на 60 минут — 56
28. Глава 27. 12 типовых кейсов внедрения — 58
29. Глава 28. Маршрут специалиста на 30 дней — 60
30. Заключение. Не стройте робота. Стройте результат — 62
31. Приложение А. Чек-лист вопросов для B2B — 64
32. Приложение В. Техническое задание агента — 66
33. Приложение С. Негативные сценарии — 68
34. Приложение D. Технологические стеки — 70
35. Приложение Е. Словарь — 72
36. Об авторе — 74

Введение. Агент — это не чат-бот

Эта глава про общая бизнес-логика. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

LLM + tools + память + контроль. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 1. Как найти работу для агента

Эта глава про аудит повторяемой работы. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

FastAPI + PostgreSQL + webhook. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 2. Аудит через вопросы и продажи

Эта глава про квалификация клиента. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

CRM API + LLM + аналитика. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 3. Карта агента: цель, память, инструменты, контроль

Эта глава про архитектура агента. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

orchestrator + tools + audit log. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 4.

В

2

В

: агент отдела продаж

Эта глава про лиды и CRM. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

CRM + RAG + email + task queue. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 5.

В

2

В

: поддержка и сервис

Эта глава про тикеты и база знаний. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

RAG + helpdesk + OCR. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 6.

В

2

G

: документы и обращения

Эта глава про регламенты и контроль. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

local LLM + RBAC + audit. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

ИТОГ

Хороший агент — это не «умная модель». Это ограниченный исполнитель с понятной задачей, инструментами, правами, проверкой и измеримым результатом. Именно такой объект можно продать, внедрить, поддерживать и масштабировать.

Глава 7.

eCom

: товар, заказ, повторная покупка

Эта глава про каталог и клиенты. Начинать здесь нужно не с модного инструмента, а с работы, которую уже выполняет человек. Если задача повторяется, имеет цифровой след и понятный результат, у неё есть шанс стать агентским процессом.

Простая модель: вход → контекст → решение → действие → проверка → журнал → следующий шаг. Если агент только генерирует текст, это ещё не полноценный процесс. Настоящая ценность появляется, когда результат попадает обратно в бизнес-систему и запускает следующий шаг.

АУДИТ ЧЕРЕЗ ВОПРОСЫ

Что является входом процесса?

Кто сейчас выполняет работу?

Сколько раз она повторяется за день, неделю и месяц?

Сколько минут занимает одна операция?

Какие данные человек открывает перед решением?

Какие действия он делает по правилам?

Где возникают исключения?

Кто проверяет результат?

Что происходит после завершения?

Что стоит ошибка или задержка?

Какие данные нельзя передавать внешней модели?

Что агент может делать самостоятельно, а что только подготовить?

КЕЙС АУДИТА

Представим компанию из 30–100 сотрудников. Руководитель говорит: «Нам нужен ИИ». Вместо демонстрации чат-бота специалист просит показать один реальный процесс. Выясняется, что сотрудник каждый день открывает почту, таблицу, CRM и папку с документами, переносит данные и пишет одинаковое письмо. За неделю таких операций набираются десятки часов.

Правильное предложение звучит так: «Давайте автоматизируем не всю работу отдела, а первый участок. Агент соберёт входящие данные, проверит обязательные поля, подготовит черновик и создаст задачу человеку. Через две недели сравним время, ошибки и долю операций без ручного копирования». Это уже нормальный пилот.

КЕЙС ВНЕДРЕНИЯ

На первом этапе агент получает только права чтения. Он собирает данные и предлагает действие. На втором этапе добавляется создание черновиков. На третьем — ограниченное выполнение с подтверждением. Только после стабильного результата рассматривается дальнейшая автономность.

ТЕХНОЛОГИЧЕСКИЙ СТЕК

OMS/ERP + catalog DB + event bus. Для пилота этого достаточно. Если процесс растёт, добавляются очередь задач, object storage, observability, RBAC, secrets manager, тестовый набор и отдельный журнал действий.

ПРОДАЖА

Продажа строится вокруг результата. Вместо «мы сделаем вам агента» лучше сказать: «Мы разберём один процесс, посчитаем ручные операции, соберём пилот и покажем цифры». После пилота появляется основание для масштабирования.

МЕТРИКИ

Смотрите не только на качество ответа модели. Нужны время операции, стоимость операции, процент автоматизации, процент ошибок, количество эскалаций, задержка, стоимость инфраструктуры и влияние на конечный бизнес-показатель.

НЕГАТИВНЫЙ СЦЕНАРИЙ

Если модель не уверена, она не должна угадывать. Агент должен остановиться, сохранить контекст и передать задачу человеку. Если API недоступен — повторить по правилам или создать исключение. Если пользователь не имеет права — действие блокируется независимо от того, что попросил пользователь.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.